

2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-69419

(43) 公開日 平成8年(1996)3月12日

(51) Int.Cl. ⁴	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 F			
	B			
9/06	5 5 0 C	7230-5B		
	X	7230-5B		
G 0 6 K 7/00	W	7623-5B		

審査請求 未請求 請求項の数2 F D (全 8 頁) 最終頁に続く

(21) 出願番号 特願平6-230603

(22) 出願日 平成6年(1994)8月30日

(71) 出願人 000001993

株式会社島津製作所

京都府京都市中京区西ノ京桑原町1番地

(72) 発明者 桒中 孝則

京都市中京区西ノ京桑原町1番地 株式会社島津製作所三条工場内

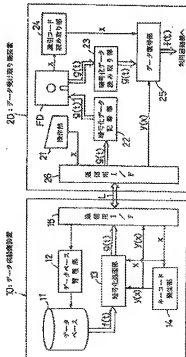
(74) 代理人 弁理士 杉谷 勉

(54) 【発明の名称】 デジタルデータの記録装置および記録媒体

(57) 【要約】

【目的】 デジタルデータの違法コピーを有効に防止することができるデジタルデータの記録装置および記録媒体を提供する。

【構成】 データ供給側装置10では、データベース11に記録されたデジタルデータを、キーコード発生部14で発生させたキーコードyと、装置20から送られてきた記録媒体FD面有の識別コードxとを使って暗号化する。データ受け取り側装置20では暗号化データを記録媒体FDに記録する。記録媒体FDから読み出された暗号化データは、装置10から与えられたキーコードyと、識別コード読み取り部24で読み取られた記録媒体FDの識別コードxとを使ってデータ復号部25で復号される。記録媒体FDの識別コードは書き換え不能に記録媒体FDに記録されている。



【特許請求の範囲】

【請求項 1】 デジタルデータを記憶するデータ記憶手段と、所望のデジタルデータを記録しようとする記録媒体固有の識別コードを入力する識別コード入力手段と、任意のキーコードを発生するキーコード発生手段と、前記データ記憶手段から読み出されたデジタルデータを前記識別コードと前記キーコードとを使って暗号化する暗号化手段と、前記暗号化されたデジタルデータ（暗号化データ）および前記キーコードを出力する出力手段と、前記暗号化データを入力する暗号化データ入力手段と、前記キーコードを入力するキーコード入力手段と、前記入力された暗号化データを記録媒体に記録する暗号化データ記録手段と、前記記録媒体に記録された暗号化データを読み取る暗号化データ読み取り手段と、前記記録媒体固有の識別コードをその記録媒体自身から読み取る識別コード読み取り手段と、前記記録媒体から読み取られた暗号化データを、前記記録媒体自身から読み取られた識別コードと前記入力されたキーコードとを使って元のデジタルデータに復号するデータ復号手段とを備えたことを特徴とするデジタルデータの記録装置。

【請求項 2】 請求項 1 に記載のデジタルデータの記録装置を使ってデジタルデータが記録される記録媒体であって、前記記録媒体には、その記録媒体固有の識別コードが書き換え不能に記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、コンピュータプログラムや音楽・映像・文字データなどのデジタルデータを記録媒体へ配給する装置、およびこの装置に使用される記録媒体に係り、特に、デジタルデータの違法コピーを防止する技術に関する。

【0002】

【従来の技術】 従来、デジタルデータの記録媒体としては例えば、磁気テープ、光磁気ディスク、半導体メモリ回路、フロッピーディスク、ハードディスクなど種々のものが知られている。コンピュータプログラムなどのデジタルデータは、この種の記録媒体に記録されて供給されたり、あるいは最近では通信回線を通じて供給されるようになっている。

【0003】 ユーザは、コンピュータプログラムを自分のコンピュータを使って他のフロッピーディスクやハードディスクなどにコピーすることができると。また、最近では、例えばコンパクトディスクのように音楽や映像情報をデジタルで記録する装置が発表されるようになってきた。

【0004】 このように、各種のソフトウェアをデジタルで記録できる装置が開発されると、ユーザは供給者から受け取ったソフトウェアを性能の変化なく、そのまま他の記録媒体にコピーすることができる。音楽や映像な

ども通信回線や放送といった手段で受け取ることができ、供給者はコンパクトディスクなどの記録媒体なしでソフトウェアを供給することができる。これにより、ソフトウェアの供給コストが下がるとともに、資源節約というメリットなどが期待される。

【0005】

【発明が解決しようとする課題】 しかしながら、デジタルデータを記録する装置は、ソフトウェアの違法コピーという問題を生む。コンピュータプログラムでは既に違法コピーが社会問題となっている。

【0006】 ソフトウェア供給者の立場から見ると、開発したソフトウェアが無断コピーによって流通してしまうと開発コストを回収できない。その結果としてソフトウェアの販売価格を高く設定せざるを得なくなる。

【0007】 一方、違法コピーをするユーザの立場から見ると、『ソフトウェアが高額過ぎる』、『書籍のように内容を確かめてから購入することができないので、正規に購入すると劣悪なソフトウェアにも優秀なソフトウェアにも同様に高い金額を支払ってしまう』などの問題意識をもっており、思わずコピーに走ってしまうという悪循環状態になっている。

【0008】 違法コピーを法的に取り締まろうとする動きもあるが、実際には違法コピーをいちいち発見することは現実的にはできないので効果に疑問がある。コンピュータソフトでは、違法コピー対策としてコピープロテクト機能をつけた形で供給などが現在行われている。音楽などの記録装置では、違法コピー対策として、記録されたデータはオリジナルデータよりも音質などが劣化するような機能を付けることが真剣に検討されている。また、コピー回数を制限するような機能を付けることなども検討されている。

【0009】 これらのように、コピーを禁止するような機能やコピー時にソフトウェアの質が変化するような機能は、デジタル記録装置の特性である『劣化なくオリジナルソースを記録できる』という長所をみすみす殺すことになっている。また、記録媒体なしに供給者がユーザにソフトウェアを供給することができるという社会的効果も期待できない。また正当にソフトウェアを利用しようとするユーザの立場から見ると、これらの機能は不便そのものである。

【0010】 この発明は、このような事情に鑑みてなされたものであって、違法コピーを有効に防止することができるデジタルデータの記録装置、およびこの装置に用いられる記録媒体を提供することを目的としている。

【0011】

【課題を解決するための手段】 この発明は、このような目的を達成するために、次のような構成をとる。すなわち、請求項 1 に記載のデジタルデータの記録装置は、デジタルデータを記憶するデータ記憶手段と、所望のデジタルデータを記録しようとする記録媒体固有の識別コー

ドを入力する識別コード入力手段と、任意のキーコードを発生するキーコード発生手段と、前記データ記憶手段から読み出されたデジタルデータを前記識別コードと前記キーコードとを使って暗号化する暗号化手段と、前記暗号化されたデジタルデータ（暗号化データ）および前記キーコードを出力する出力手段と、前記暗号化データを入力する暗号化データ入力手段と、前記キーコードを入力するキーコード入力手段と、前記入力された暗号化データを記録媒体に記録する暗号化データ記録手段と、前記記録媒体に記録された暗号化データを読み取る暗号化データ読み取り手段と、前記記録媒体固有の識別コードをその記録媒体自身から読み取る識別コード読み取り手段と、前記記録媒体から読み取られた暗号化データを、前記記録媒体自身から読み取られた識別コードと前記入力されたキーコードとを使って元のデジタルデータに復号するデータ復号手段とを備えたものである。

【0012】請求項2に記載の記録媒体は、請求項1に記載のデジタルデータの記録装置を前記記録媒体には、その記録媒体固有の識別コードが書き換え不能に記録されている。

【0013】

【作用】請求項1に記載の発明の作用は次のとおりである。ユーザが所望のデジタルデータの供給を受けようとする場合、そのデジタルデータを記録しようとする記録媒体固有の識別コードが識別コード入力手段を介して入力される。データ記憶手段から取り出されたデジタルデータは、前記識別コードとキーコード発生手段から発生されたキーコードとを使って、暗号化手段によって暗号化される。暗号化されたデジタルデータ（暗号化データ）とキーコードとが出力手段を介して出力される。この暗号化データは暗号化データ入力手段を介して取り込まれ、暗号化データ記録手段によって前記識別コードをもつ記録媒体に記録される。そのデジタルデータを利用する場合には、暗号化データ読み取り手段によって記録媒体から暗号化データが読み取られてデータ復号手段に送られる。そして、識別コード読み取り手段によってその記録媒体自身から読み取られた識別コードとキーコード入力手段を介して入力されたキーコードとを使って、暗号化データが復号される。

【0014】請求項2に記載の発明によれば、暗号化データが記録された記録媒体（第1記録媒体）から別の記録媒体（第2記録媒体）へ暗号化データをコピーしたとしても、第2記録媒体の識別コードを第1記録媒体と同じ識別コードに書き換えることができないので、請求項1の装置を使っても第2記録媒体にコピーされた暗号化データを復号することはできない。

【0015】

【実施例】以下、図面を参照してこの発明の一実施例を説明する。

＜第1実施例＞図1は、この発明に係るデジタルデータの記録装置の第1実施例の概略構成を示したブロック図である。

【0016】この実施例装置は、データ供給側装置10とデータ受け取り側装置20とから構成され、両装置間が通信回線Lで接続されている。データ供給側装置10は、ソフトウェアを販売する販売会社などに設置されるものである。一方、データ受け取り側装置20は、ソフトウェアを利用するユーザ側に設置されるもので、通常、一つのデータ供給側装置10に対して多数のデータ受け取り側装置20が通信回線Lを介して結ばれるが、図1では簡単のために一つのデータ受け取り側装置20のみを示している。なお、各装置10、20の設置場所は任意であり、上記の例以外に、データ供給側装置10をソフトウェア・メーカーに、データ受け取り側装置20をソフトウェア販売店にそれぞれ設置し、ユーザがソフトウェア販売店に向いて所望のソフトウェアの供給を受けるようにしてもよい。以下、各装置10、20の詳細な構成を説明する。

【0017】データ供給側装置10は、販売対象となる多種類のソフトウェアを格納したデータベース11、データベース11を管理するデータベース管理部2、供給要求のあったソフトウェア（デジタルデータ）を暗号化する暗号化処理部13、暗号化のための任意のキーコードを発生するキーコード発生部14、通信用インターフェース（I/F）15などから構成されている。ここで、通信用インターフェース15は本発明における識別コード入力手段および出力手段に相当している。

【0018】データ受け取り側装置20は、データ要求指令や記録媒体FDの識別コードなどを入力するためのキーボードなどからなる操作部21、データ供給側装置10から送られてきた暗号化データを記録媒体FDに記録するための暗号化データ記録部22、記録媒体FDから暗号化データを読み取るための暗号化データ読み取り部23、記録媒体FDから識別コードを読み取るための識別コード読み取り部24、暗号化データを復号するためのデータ復号部25、通信用インターフェース26などから構成されている。ここで、通信用インターフェース26は本発明における暗号化データ入力手段およびキーコード入力手段に相当している。

【0019】記録媒体FDは、特にその種類を限定しないが、例えばフロッピーディスク、磁気テープ、光磁気ディスク、半導体メモリ回路、ハードディスクなどが用いられる。この記録媒体FDには、その記録媒体固有の識別コードが書き換え不能に予め記録されている。識別コードの記録手法は特に限定しないが、例えば、ユーザが書き換えできない領域（プロテクト領域）に識別コードを磁気的に記録しておいたり、あるいはフロッピーディスクの円盤状磁気シートが収納されたジャケット表面にバーコードを書き換え不能に記録しておく。このような

記録媒体固有の識別コードは例えば、その記録媒体を製造するメーカーが出荷段階で、各記録媒体ごとに例えば連続番号などの形態で記録しておく。

【0020】次に上述した実施例装置を使ってソフトウェアの供給を受ける場合の動作を図2のフローチャートを参照して説明する。なお、図2の各ステップ番号の添字中、Sはデータ供給側装置10での処理、Uはデータ受け取り側装置20での処理をそれぞれ示している。

【0021】まず、ユーザが、データ受け取り側装置20の操作部21を使って、希望するソフトウェアのデータ要求と、そのデータを記録しようとする記録媒体FDの識別コードとを入力する(1U)。この入力情報は通信回線Lを介してデータ供給側装置10に送られる。なお、記録媒体FDの識別コードは、識別コード読み取り部24で読み取ったものをデータ供給側装置10に送るようにしてもよい。

$$y(x) = x^3 + Ex^2 + Fx$$

上式①でE、Fは任意定数である。

【0025】また、暗号化データg(t)を次式②で示

$$g(t) = h(f, x, y)$$

$$= \{f(t) + A\} \{x^2 + Bx + C\} + Dy + G \quad \text{.....②}$$

上式②で、A、B、C、D、Gは任意定数である。

【0026】上記のように各関数を設定すると、暗号化

$$g(t) = \{f(t) + A\} \{x^2 + Bx + C\} + D \{x^3 + Ex^2 + Fx\} + G \quad \text{.....③}$$

【0027】上記のようにして暗号化されたデータg(t)と、キーコードy(x)とを通信回線Lを介してデータ受け取り側装置20に伝送する(4S)。

【0028】データ受け取り側装置20では、伝送されてきた暗号化データを暗号化データ記録部22が記録媒体FDにそのまま記録するとともに、キーコードをデータ復号部25に蓄積する(5S)。

【0029】記録媒体FDに記録されたデータを利用する場合は、暗号化データ読み取り部23が記録媒体FDから暗号化データを読み出してデータ復号部25に送る(6U)。

【0030】また、識別コード読み取り部24が記録媒

$$f(t) = h^{-1}(g, x, y)$$

$$= \{ \{g(t) - G - Dy\} / \{x^2 + Bx + C\} \} - A$$

.....④

上式④の逆関数にデータ供給側装置10から送られてきたキーコードyと、識別コード読み取り部24で読み取られた識別コードxの値を代入することにより元のデ

$$f(t) = \{ \{g(t) - G - D \{x^3 + Ex^2 + Fx\} \} / \{x^2 + Bx + C\} \} - A \quad \text{.....⑤}$$

【0033】以上のようにして復号されたデジタルデータf(t)は、データ受け取り側装置20の図示しない利用回路へ送られる。

【0034】次に上述した実施例装置で違法コピーを有効に防止できることを説明する。仮に、上記の処理によ

【0022】データ供給側装置10では、データベース管理部12がデータ受け取り側装置20からのデータ要求に基づき、要求のあったソフトウェアのデジタルデータをデータベース11から取り出して暗号化処理部13に送る(2S)。

【0023】暗号化処理部13は、前記デジタルデータをデータ受け取り側装置20から送られてきた識別コードと装置10内のキーコード発生部14で発生されたキーコードとを使って暗号化する(3S)。

【0024】デジタルデータの暗号化処理の簡略化した例を以下に説明する。いま、暗号化処理されるデジタルデータをF(t)、記録媒体FDの識別コードをx、キーコードをy(x)、暗号化データをg(t)で表す。例えば、キーコードy(x)を次式①で表される関数に設定する。

.....①

される関数h(f, x, y)とする。

データg(t)は、上記②式にキーコードの関数yを代入して、次式③のようになる。

体FDに記録された識別コードを、記録媒体FD自身から読み取り、その識別コードをデータ復号部25に送る(7U)。

【0031】データ復号部25は、記録媒体FDから読み取られた暗号化データを、データ供給側装置10から送られてきたキーコードと、識別コード読み取り部24で読み取られた識別コードとを使って、元のデジタルデータに復号する(8U)。

【0032】この復号処理を上記の簡略化された例で説明すれば以下のようになる。データ復号部25は、暗号化データを復号するための、次式④で表される逆関数h⁻¹(g, x, y)をもっている。

ジタルデータf(t)が復号される。すなわち、元のデジタルデータf(t)は次式⑤で再現される。

り所定の記録媒体FD(以下、第1記録媒体という)に暗号化データが記録され、この第1記録媒体から別の記録媒体(以下、第2記録媒体という)にその暗号化データがコピーされたとする。その第2記録媒体を実施例のデータ受け取り側装置20にセッティングして復号し

ようとした場合、識別コード読み取り部 24 で読み取られる第 2 記録媒体の識別コードは第 1 記録媒体の識別コードとは異なったものになる。したがって、その識別コードをデータ復号部 25 に渡しても、第 1 記録媒体の識別コードを使って暗号化された暗号化データを復号することができないのである。

【0035】<第 2 実施例>次に、供給されたデジタルデータをユーザ側で適法にコピーするための装置の例を図 3 を参照して説明する。図 3 は、適法にコピーをするための構成を追加したデータ受け取り側装置 20 の概略構成図である。図中、図 1 に示した符号と同一の符号で示した構成部分は、上述の第 1 実施例と同じ構成部分であるので、ここでの説明は省略する。また、データ供給側装置 10 も第 1 実施例と同様であるのでここでの説明は省略する。

【0036】図 3 に示したデータ受け取り側装置 20 は、供給されたデジタルデータをコピーするための構成として、データ復号部 25 で復号されたデジタルデータを新たに暗号化するための暗号化処理部 27、新たな暗号化データを別の記録媒体 F D 2 に記録するための暗号化データ記録部 28 を備えている。

【0037】最初に記録された記録媒体 F D 1 から別の記録媒体 F D 2 にデータをコピーしたい場合、ユーザはデータ受け取り側装置 20 の操作部 21 を使って、データ供給側装置 10 にデータコピーの要求と記録媒体 F D 2 の識別コード x_2 を送る。この要求に基づきデータ供給側装置 10 は、新たなキーコード y_2 (x_2) をデータ受け取り側装置 20 へ送る。このキーコード y_2 はデータ受け取り側装置 20 の暗号化処理部 27 に与えられる。また、ユーザは操作部 21 を使って新たな記録媒体 F D 2 の識別コード x_2 を入力する。この識別コード x_2 は暗号化処理部 27 に与えられる。暗号化処理部 27 は、キーコード y_2 と識別コード x_2 を使って、データ復号部 25 から出力されたデジタルデータを再度、暗号化する。新たな暗号化データ g_2 は暗号化データ記録部 28 によって記録媒体 F D 2 に記録される。

【0038】以上のようにしてコピーされた記録媒体 F D 2 を、元の記録媒体 F D 1 に変えてデータ受け取り側装置 20 にセッティングすれば、データ復号部 25 がキーコード y_2 と識別コード読み取り部 24 で読み取られた記録媒体 F D 2 の識別コード x_2 を使って記録媒体 F D 2 の暗号化データ g_2 を復号することにより、コピーされたデジタルデータ f を利用することができる。

【0039】<第 3 実施例>図 4 および図 5 を参照する。図 4 はデータ供給側装置の概略構成を示したブロック図、図 5 はデータ受け取り側装置の概略構成を示したブロック図である。

【0040】図 4 に示したデータ供給側装置は、例えばソフトウェア販売店などに設置されるもので、暗号化されたデジタルデータ g を記録媒体 F D に記録する暗号化

データ記録部 22 を備えている。ユーザが、あるソフトウェアの購入を希望すると、操作部 21 A からそのソフトウェアが指定される。指定されたソフトウェアのデジタルデータは、操作部 21 A から入力された記録媒体 F D の識別コード x と、キーコード発生部 14 から発生されたキーコード y を使って暗号化処理部 13 で暗号化される。暗号化されたデジタルデータ g はインターフェース 17 を介して暗号化データ記録部 22 に与えられ、この暗号化データ記録部 22 で記録媒体 F D に記録された後にユーザに手渡される（販売される）。暗号化データを解読するためのキーコード y はプリンタ 16 で印字出力されユーザに手渡される。

【0041】ソフトウェアを購入したユーザは図 5 に示したデータ受け取り側装置によって暗号化データを復号する。すなわち、データ受け取り側装置では、記録媒体 F D の識別コード x が識別コード読み取り部 24 によって読み取られるとともに、操作部 21 B を介してユーザによってキーコード y が入力される。データ復号部 25 は、上述した識別コード x とキーコード y を使って暗号化データ g を復号し、利用回路部 26 に出力する。

【0042】

【発明の効果】以上の説明から明らかなように、この発明によれば次の効果を奏する。請求項 1 に記載のデジタルデータの記録装置によれば、任意のキーコードと記録媒体固有の識別コードとを使って暗号化されたデジタルデータが、その識別コードをもった記録媒体に記録されるので、その記録媒体（第 1 記録媒体）に記録された暗号化データを別の記録媒体（第 2 記録媒体）にたとえコピーしても、第 2 記録媒体の識別コードは第 1 記録媒体の識別コードとは異なるので、第 2 記録媒体にコピーされた暗号化データを復号することができない。したがって、この装置によればデジタルデータの違法コピーを有効に防止することができる。

【0043】また、請求項 2 に記載の記録媒体によれば、記録媒体にその記録媒体固有の識別コードが書き換え不能に記録されているので、上記の例で第 2 記録媒体の識別コードを第 1 記録媒体の識別コードに書き換えることにより暗号化データを復号するということができず、デジタルデータの違法コピーの防止を確実なものにすることができる。

【図面の簡単な説明】

【図 1】第 1 実施例装置の概略構成を示したブロック図である。

【図 2】第 1 実施例装置の動作フローチャートである。

【図 3】第 2 実施例装置のデータ受け取り側装置の概略構成を示したブロック図である。

【図 4】第 3 実施例装置のデータ供給側装置の概略構成を示したブロック図である。

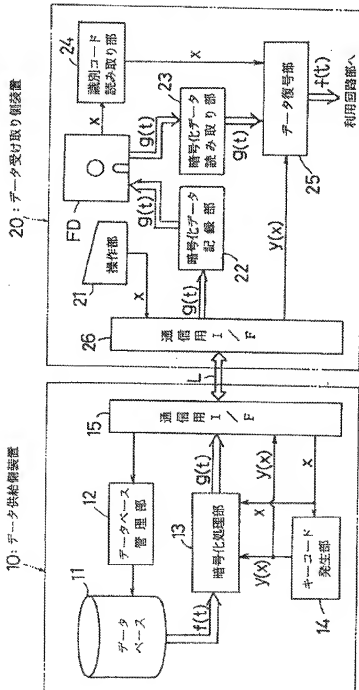
【図 5】第 3 実施例装置のデータ受け取り側装置の概略構成を示したブロック図である。

【符号の説明】

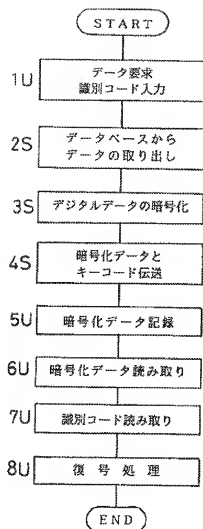
- 10…データ供給側装置
 11…データベース
 12…データ管理部
 13…暗号化処理部
 14…キーコード発生部
 15、26…通信用インターフェース
 20…データ受け取り側装置

- 21…操作部
 22…暗号化データ記録部
 23…暗号化データ読み取り部
 24…識別コード読み取り部
 25…データ復号部
 FD…記録媒体

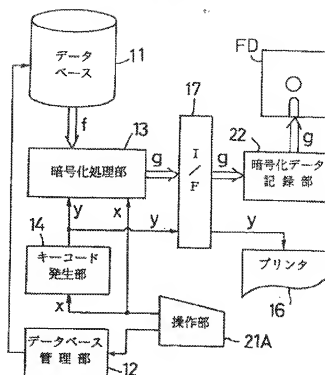
【図1】



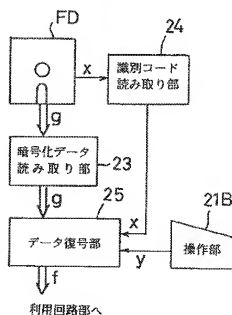
【図2】



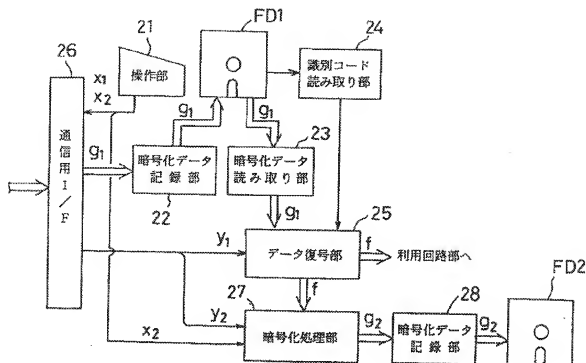
【図4】



【図5】



【図 3】



フロントページの続き

(51) Int. Cl. 6

G 0 6 K 17/00

G 0 9 C 1/00

識別記号 庁内整理番号

S

7259-5J

F I

技術表示箇所

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-069419

(43)Date of publication of application : 12.03.1996

(51)Int.Cl.

G06F 12/14

G06F 9/06

G06K 7/00

G06K 17/00

G09C 1/00

(21)Application number : 06-230603

(71)Applicant : SHIMADZU CORP

(22)Date of filing : 30.08.1994

(72)Inventor : NONAKA TAKANORI

(54) RECORDING DEVICE AND RECORDING MEDIUM FOR DIGITAL DATA

(57)Abstract:

PURPOSE: To provide the recording device and recording medium for digital data which can effectively prevent the digital data from illegally being copied.

CONSTITUTION: A data-supply side device 10 encodes the digital data recorded in a data base 11 by using a key code (y) generated by a key code generation part 14 and the identification code (x) which is characteristics of the recording medium FD and sent from a device 20. A data-reception side device 20 records the encoded data on the recording medium FD. The encoded data read out of the recording medium FD are decoded by a data decoding part 25 by using the key code (y) supplied from the device 10 and the identification code (x) of the recording medium FD which is read out by an identification code read part 24. The identification code on the recording medium FD is recorded on the recording medium FD in an unwritable state.

